REMARKS

Reconsideration of this Application is respectfully requested. In response to the Office Action mailed February 25, 2005, Applicant has amended claim 25. Claims 1-27 are pending.

Based on the above Amendment and the following Remarks, Applicant respectfully requests that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Request for Acknowledgement of Figures

In the Preliminary Amendment filed September 24, 2002, Applicant submitted new figures 1-6 replacing the figures as filed. Applicant respectfully requests that the Examiner consider these figures.

Rejections under 35 U.S.C. § 103

On pages 2-4, the Action rejects claims 1-9 and 15-19 under 35 U.S.C. § 103(a) as being unpatentable over Applied Cryptography, Second Edition to Schneier (hereinafter "Schneier") in view of U.S. Patent No. 6,175,924 to Arnold (hereinafter "Arnold"). Applicant notes that the Action does not apply a rejection to claim 19 in this section, and instead applies a rejection in view of different references on page 6 of the Action (see section (C) below). Applicant believes listing claim 19 as being rejected over Scheier and Arnold was an inadvertent error.

Applicant respectfully traverses the rejection of claims 1-9 and 15-18 as the Action fails to establish a *prima facie* case of obviousness. In order to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. M.P.E.P. § 2143.

(A) For at least the following three reasons, the Action does not establish a *prima facie* case of obviousness to reject claim 1 in view of the combined teachings of Schneier and Arnold.

Claim 1 recites: "A method for transferring a first electronic key between a key provider system and a second other system via an information network comprising the steps of: a) encrypting the first electronic key using a first encryption key of the key provider; b) providing within the second other system a first secure module having a second encryption key within a read-only memory circuit thereof and provided with the first secure module, the second encryption key accessible only by program code being executed on a processor internal to the first secure module, and wherein the second encryption key is other than modifiable and other than accessible outside of the module; c) transferring the encrypted first electronic key from the key provider system to the second other system via the information network; d) providing the encrypted first electronic key to the processor internal to the first secure module of the second other system; and, e) executing program code on the processor internal to the first secure module to decrypt the encrypted first electronic key using the second encryption key stored within the read-only memory circuit of the first secure module and to store the decrypted first electronic key internally within a secure key memory location of the first secure module" (emphasis added).

First, Schneier and Arnold do not teach or suggest "providing within the second other system a first secure module having a second encryption key within a read-only memory circuit," as recited in claim 1. As correctly admitted in the Action on page 3, Schneier does not teach or suggest a "ROM," and therefore does not teach or suggest "a second encryption key within a read-only memory circuit." Likewise, Arnold does not teach or suggest "a first secure module having a second encryption key within a read-only memory circuit," as recited in claim 1. Instead, in FIG. 2, Arnold discloses a private key K_{PR} stored in a secure persistent storage that is attached to a ROM 55, but does not disclose the private key K_{PR} being stored within the ROM 55 (see Arnold, FIG. 2, col. 4, lines 50-52, 58-59, col. 5, lines 31-33). Thus, Schneier and Arnold do not teach or suggest "providing within the second other system a first secure module having a second encryption key within a read-only memory circuit," as recited in claim 1.

Second, Schneier and Arnold do not teach or suggest "a secure encryption key accessible only by program code being executed on a processor internal to the first secure module," as recited in claim 1. As admitted in the Action on page 3, Schneier "fails to disclose the encrypting and decrypting being performed in a secure module containing a processor." Therefore, Schneier does

not teach of suggest "a secure encryption key accessible only by program code being executed on a processor internal to the first secure module," as recited in claim 1.

Likewise, Arnold does not teach of suggest "a secure encryption key accessible only by program code being executed on a processor internal to the first secure module," as recited in claim 1. On page 3, the Action relies on column 3, lines 48-61 of Arnold for a teaching of "a secure module with such features." However, for the following reasons, while Arnold may disclose using private key/public key pairs, Arnold does not teach or suggest that either the private key or the public key is accessible "only by program code being executed on a processor internal to the first secure module."

Arnold discloses a system for certifying the authenticity of an application program to prevent certified applications programs from accessing data that is not their own (see Arnold, Abstract). Arnold discloses a computer program 35 used to allocate memory segments to applications programs so that a memory segment allocated to one application program cannot be viewed or allocated by another application program (see Arnold, col. 4, lines 25-39). The program 35 may be employed on a security card 11. The program 35 may be implemented as a special purpose apparatus by storing the program's executable instructions in RAM 53, ROM 55, or a combination of both and/or loaded into RAM 53 from a hard disk drive (DASD) 27 (see Arnold, FIG. 1, col. 3, lines 47-56). RAM 53 and ROM 55 contain the operating system, and the ROM 55 is attached to a persistent memory 107 (see Arnold, FIG. 2, col. 4, lines 50-57). The security card 11 includes a cryptographic processing module 57 and a processor 51 (see Arnold, FIG. 1, col. 3, lines 55-61). The persistent storage stores a private key K_{PR} that is used to encrypt a hash of a unique application program name N_A and of the application program P_A to determine the digital signature DSIG. K_{PR} is the private key of a public/private key pair with public key K_{PU} (see Arnold, col. 5, lines 31-38). The public key K_{PU} is made available at multiple computer systems (see Arnold, col. 5, lines 35-38). The DSIG may be calculated using Rivest Shamir & Adleman (RSA), which is known to process public and private keys.

However, Arnold does not teach or suggest that either of the private key or the public key are "accessible only by program code being executed on a processor internal to the first secure module." The main idea of Arnold is to allocate memory segments to a particular application

program, and then protect the memory segments from modification by other application programs that are not allocated to that particular application program (see Arnold, col. 4, lines 8-49). Nevertheless, the concept of limiting key access only to program code on a processor internal within a secure module is not even discussed in Arnold. Although the private key K_{PR} of Arnold is stored in secure persistent storage (see Arnold, col. 5, 31-34), this does not imply that program code on an authorized *external* processor cannot access the private key K_{PR}. The secure persistent storage prevents unauthorized access of the private key K_{PR}, and Arnold does not state that program code from an authorized processor external to the security card cannot access the private key K_{PR}. Thus, Arnold does not teach or suggest "a secure encryption key accessible only by program code being executed on a processor internal to the first secure module," as recited in claim 1.

Third, Schneier and Arnold do not teach or suggest "wherein the second encryption key is other than modifiable and other than accessible outside of the module," as recited in claim 1. As correctly admitted on page 3 of the Action, Schneier does not teach or suggest any such feature. Likewise, Arnold does not teach or suggest that the private key K_{PR} or the public key K_{PU} is other than modifiable and other than accessible outside of the security card 11. Although the private key K_{PR} is stored in secure persistent storage, the secure persistent storage is to prevent unauthorized access. Arnold does not teach that external processors cannot be authorized to modify or access the private key K_{PR} in the secure persistent storage. Likewise, the public key K_{PU} of Arnold is "made available at every computer system where the authority expects programs certified with K_{PR} to be used" (see Arnold, col. 5, lines 35-38). Thus, the public key K_{PU} is modifiable and accessible outside of the security card 11. Therefore, Arnold does not teach or suggest "wherein the second encryption key is other than modifiable and other than accessible outside of the module," as recited in claim 1.

Accordingly, the Action does not establish a *prima facie* case of obviousness for using the combined teachings Schneier and Arnold to reject claim 1 as these references do not teach or suggest all of the claim features. Applicant respectfully requests that the rejection be withdrawn.

Therefore, claim 1 is in condition for allowance and allowance thereof is respectfully requested.

Claims 2-9, which depend from claim 1, are also in condition for allowance due to their dependence on an allowable claim.

Claim 15 is in condition for allowance for reasons analogous to those given for claim 1. More specifically, the combined teachings of Schneier and Arnold do not teach or suggest "the at least a first encryption key being other than accessible by any code other than the program code and being other than modifiable thereby," as recited in claim 15. Therefore, claim 15 is allowable over the applied references and allowance thereof is respectfully requested.

Claims 16-18, which depend from claim 15, are also in condition for allowance due to their dependence on an allowable claim.

(B) On pages 4-6, the Action rejects claims 10-14 and 21-24 under 35 U.S.C. § 103(a) as being unpatentable over Schneier and Arnold, in further view of U.S. Patent No. 5,680,458 to Spelman et al. (hereinafter "Spelman").

Claim 10 is in condition for allowance for reasons analogous to those given for claim 1. Specifically, Scheier, Arnold, and Spelman do not teach or suggest "the second and third encryption keys accessible only by program code being executed on a processor internal to the first secure module," and "wherein the second and third encryption keys are other than accessible outside of the module," as recited in claim 10. Spelman is not relied upon for a teaching of these features, and in fact, does not teach or suggest any such features. Therefore, claim 10 is allowable over the applied references and allowance thereof is respectfully requested.

Claims 11-14, which depend from claim 10, are also in condition for allowance due to their dependence on an allowable claim.

Claim 21 is in condition for allowance for reasons analogous to those given for claim 1. Additionally, Arnold, and Spelman do not teach or suggest "decrypting the encrypted third encryption key using one of the first and second encryption keys and for storing the decrypted third encryption key approximately within the same memory location of the other one of the first and second encryption keys," and "the first and second encryption keys being other than accessible by

any code other than the program code and being other than modifiable absent erasing thereof by any code other than the program code." Spelman is not relied upon for a teaching of these features, and in fact, does not teach or suggest any such features. Therefore, claim 21 is allowable over the applied references and allowance thereof is respectfully requested.

Claims 22-24, which depend from claim 21, are also in condition for allowance due to their dependence on an allowable claim.

(C) On page 6, the Action rejects claim 19 under 35 U.S.C. § 103(a) as being unpatentable over Schneier and Arnold, in further view of U.S. Patent No. 5,559,889 to Easter et al. (hereinafter "Easter").

Claim 19 depends from allowable claim 15, and is therefore in condition for allowance.

(D) On pages 6-7, the Action rejects claim 20 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Arnold, and Easter, in further view of U.S. Patent No. 5,249,277 to Bergum et al. (hereinafter "Bergum").

Claim 20 depends from allowable claim 15, and is therefore in condition for allowance.

(E) On pages 7-8, the Action rejects claim 25 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Arnold, and Spellman, in further view of U.S. Patent No. 4,386,234 to Ehrsam et al. (hereinafter "Ehrsam").

Claim 25 depends from allowable claim 21, and is therefore in condition for allowance.

(F) On pages 8-9, the Action rejects claim 26 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Arnold, Spellman, and Ehrsam, in further view of Easter.

Claim 26 depends from allowable claim 21, and is therefore in condition for allowance.

(G) On page 9, the Action rejects claim 27 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Arnold, and Easter, in further view of Bergum.

Claim 27 depends from allowable claim 21, and is therefore in condition for allowance.

Therefore, claims 1-27 are in condition for allowance and allowance thereof is respectfully requested.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is hereby invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment is respectfully requested.

Respectfully submitted,

Date June 27, 2005

Edward W. Yee
Registration No. 47,294
VENABLE, LLP
P.O. Box 34385
Washington, D.C. 20043-9998
Telephone: (202) 344-4000
Telefax: (202) 344-8300